RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: DSA-W09

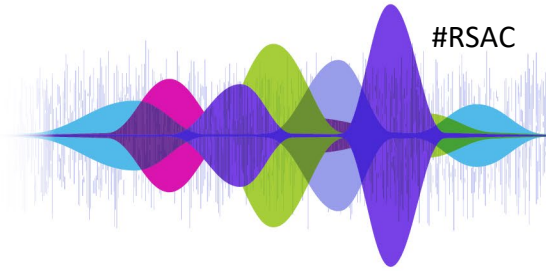
Application of Cyber-Informed Engineering to Municipal Utility Security

Virginia Wright

Cyber-Informed Engineering Program Manager
Idaho National Laboratory
https://www.linkedin.com/in/virginia-l-wright/

Marcus H. Sachs, P.E.

SVP and Chief Engineer
Center for Internet Security
https://www.linkedin.com/in/marcsachs/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Cybersecurity Threats Are Targeting Critical Infrastructure

Attackers May Be Coming for Your Plant. Time to Tighten Cyber Defenses.

The water and wastewater sectors are targets for a variety of cyber attacks. Some simple measures can go a long way to protect critical operations

Every "Thing" Everywhere All at Once

Every asset in an organization's inventory that is not accounted for and protected is a potential attack vector that an attacker can use to gain access or move undetected.

BY ANDY GREENBERG SECURITY APR 17, 2024 6:00 AM

Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities

Cyber Army of Russia Reborn, a group with ties to the Kremlin's Sandworm unit, is crossing lines even that notorious cyberwarfare unit wouldn't dare to.

Cybersecurity

US warns hackers are carrying out attacks on water systems

Russia-linked hackers claim cyberattacks on U.S., French and Polish water utilities

CYBERSECURITY ADVISORY

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Release Date: May 24, 2023 **Alert Code:** AA23-144a

Arkansas City water treatment facility hit by cyberattack

While disruptions are limited, the attack on the water treatment facility highlights how the critical infrastructure sector remains a popular target for threat actors.

By **Arielle Waldman**, News Writer Published: **24 Sep 2024**

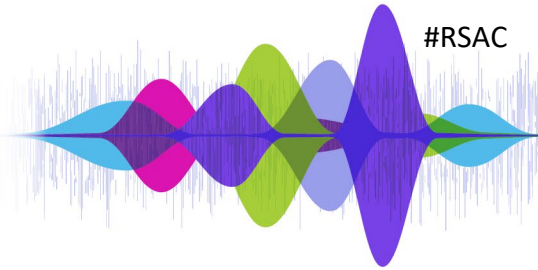
Russian hackers breached, sabotaged Texas water treatment plant, cyber firm says

RSAC™ 2025 Conference

Cybersecurity and Operational Technology

Many Voices.
One Community.

What Is Cybersecurity?



Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

-- Cybersecurity and Infrastructure Security Agency (CISA)

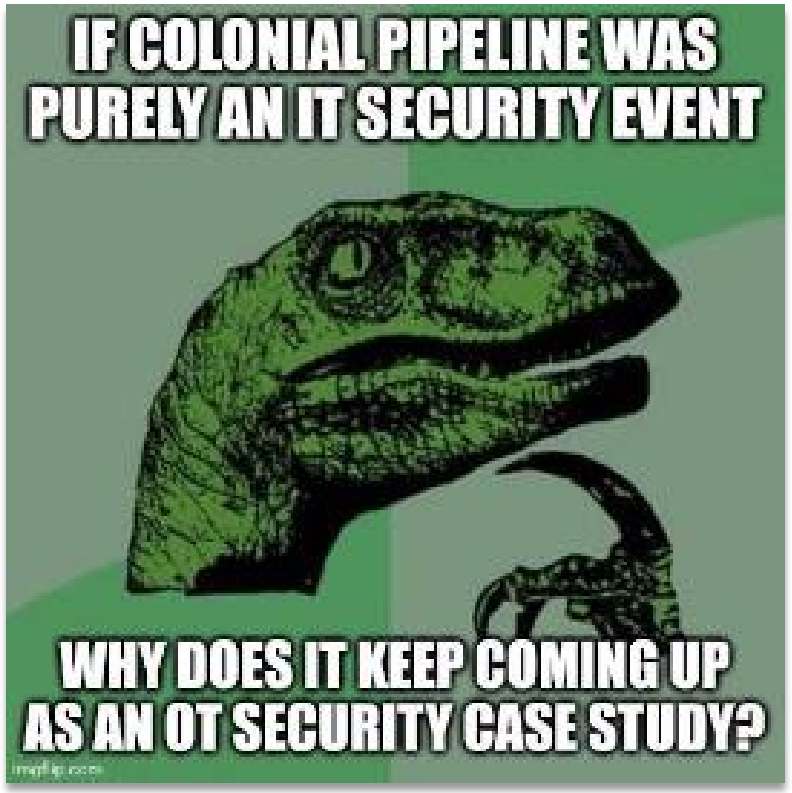
What Is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

-- Cybersecurity and Infrastructure Security Agency (CISA)

What's missing in this statement?

Cybersecurity Is Not Just About Data



Joe Slowick, MITRE

- Ransomware attacked business data on an IT network
- However, pipeline operations were curtailed
- *Why*?

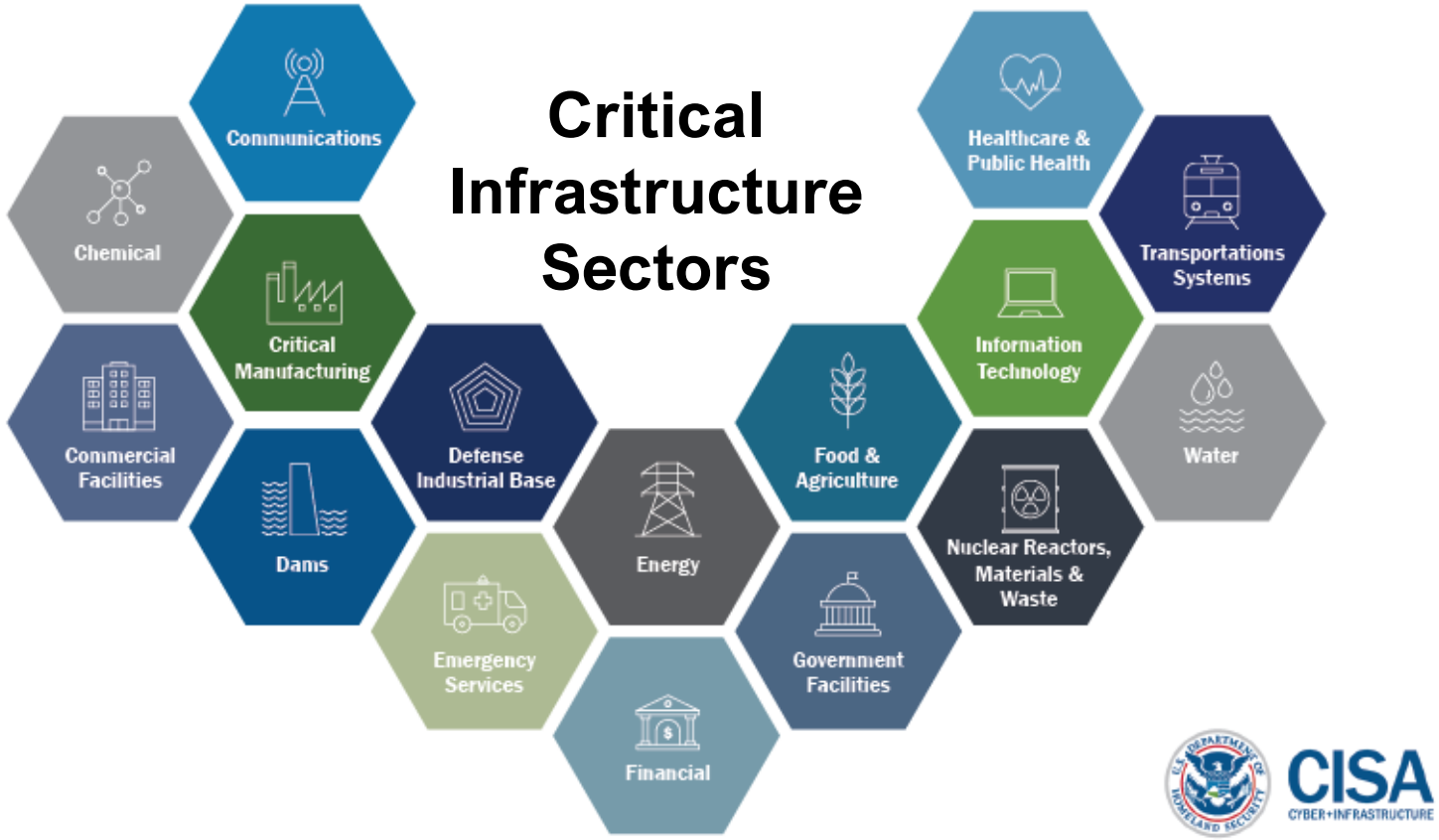
The USS John S. McCain Incident

- On Aug. 21, 2017, the USS John S. McCain collided with an oil tanker near the Strait of Malacca, resulting in the death of ten sailors and marking the Navy's worst accident in four decades
- While the Navy initially blamed the incident on the McCain's crew, later investigations pointed out problems with the ship's navigation software
- The Navy's own review of the crash stated, "There is a tendency of designers to add automation … without considering the effect to operators who are trained and proficient in operating legacy equipment"

"Ultimately … these design flaws were rooted in the proclivity of system designers to automate and digitalize navigation functions without sufficient attention to the needs of operators."

U.S. Fleet Forces Command, "Comprehensive Review of Recent Surface Forces Incidents"

What is Critical Infrastructure?

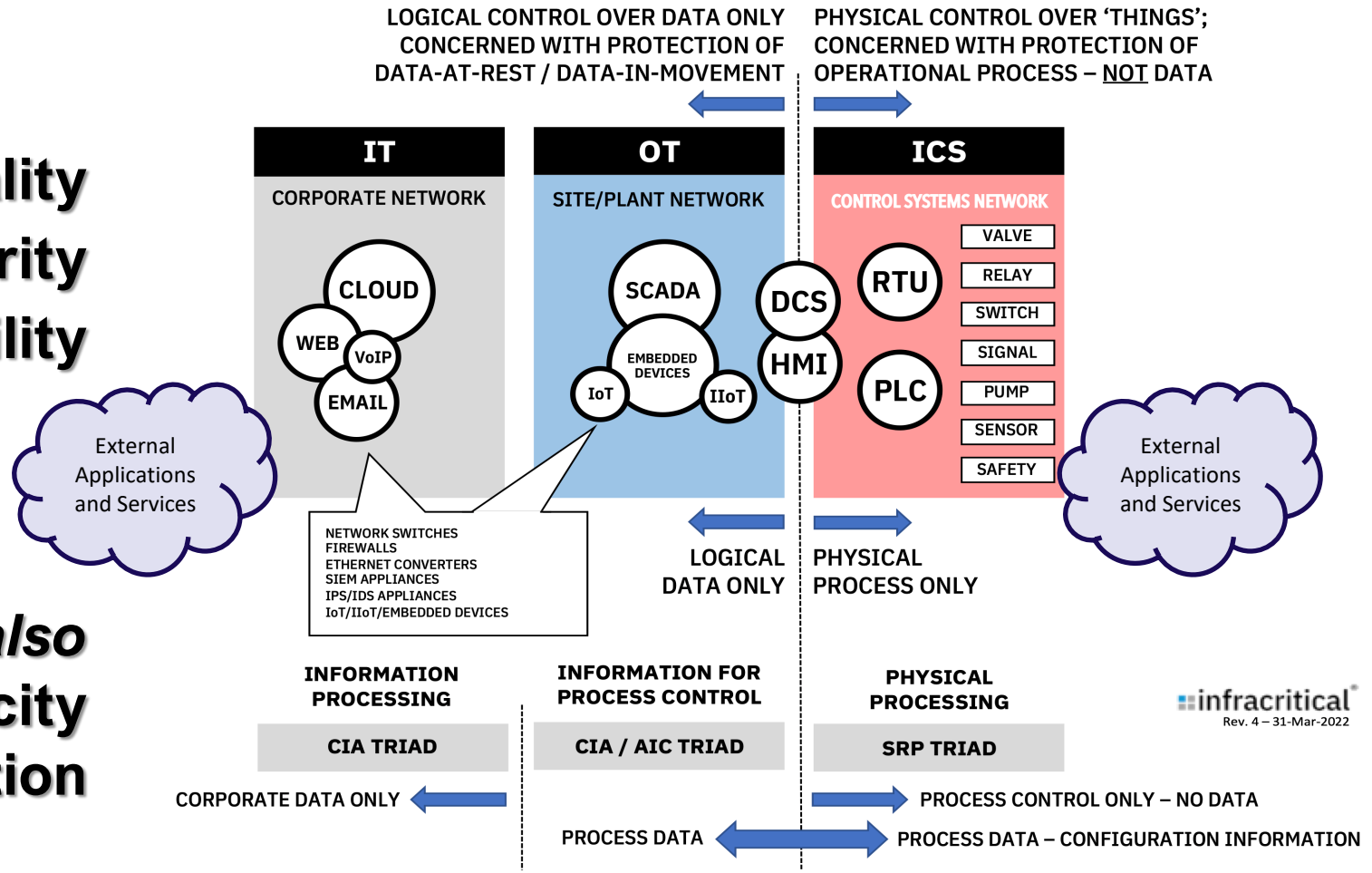


Most critical infrastructure sectors leverage both
IT – Information Technology and **OT – Operational Technology**

Information Technology (IT) vs Operational Technology (OT) vs Industrial Control Systems (ICS)

Confidentiality
Integrity
Availability

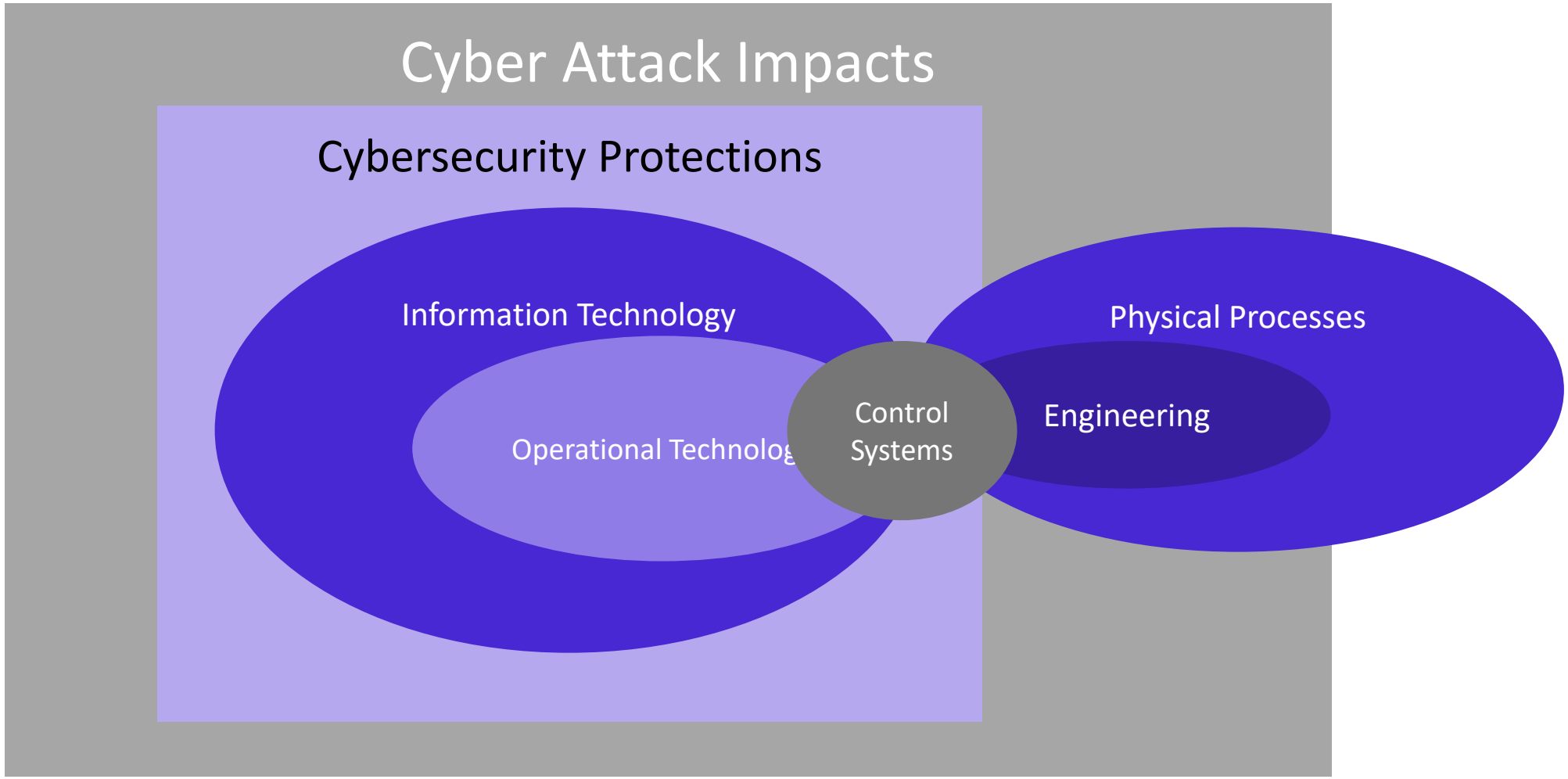
….*also*
Authenticity
Non-Repudiation



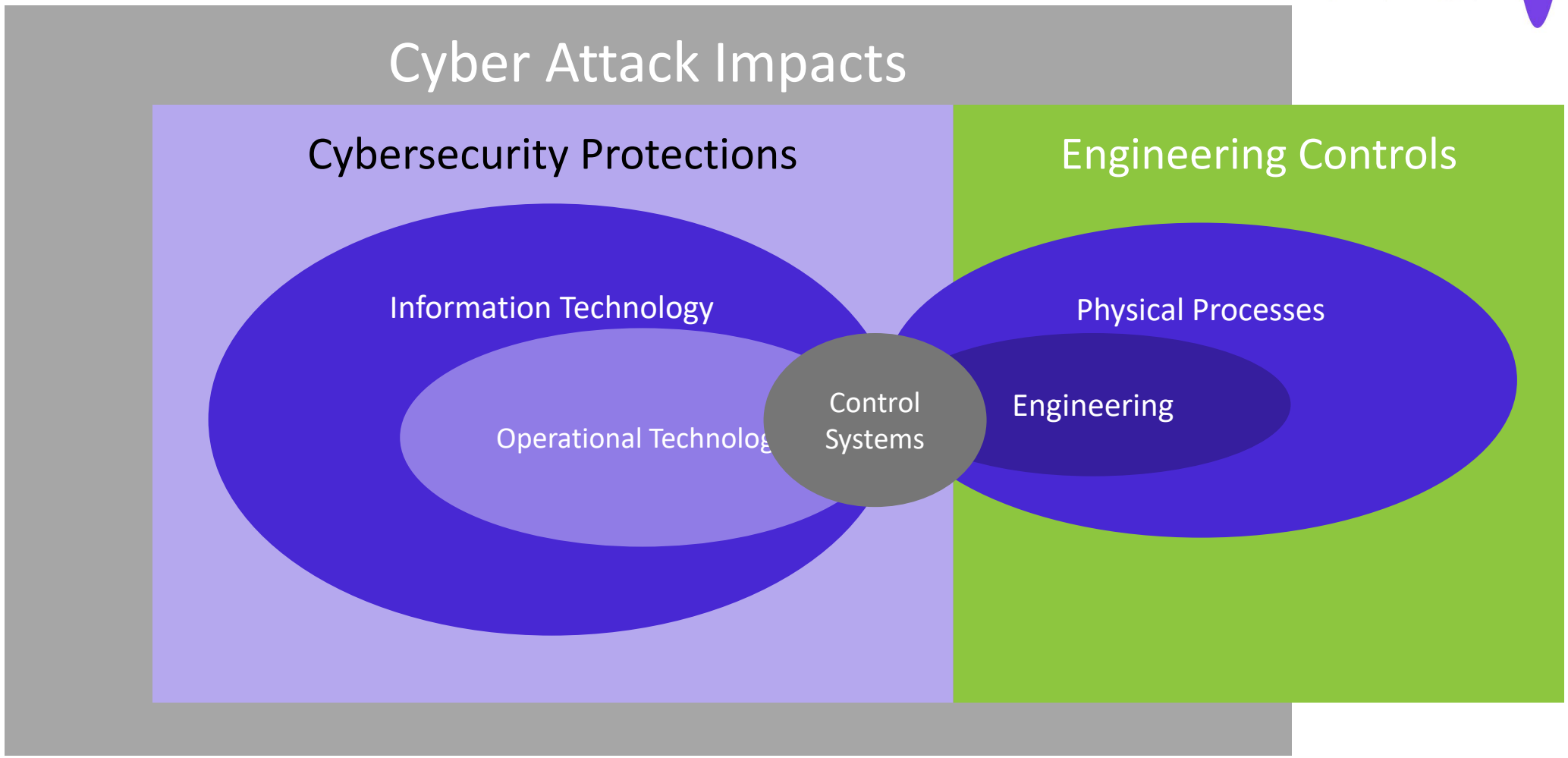
Safety
Reliability
Performance

http://icsmodel.infracritical.com/

Cybersecurity in Operational Technology



Cybersecurity in Operational Technology



RSAC™ 2025 Conference

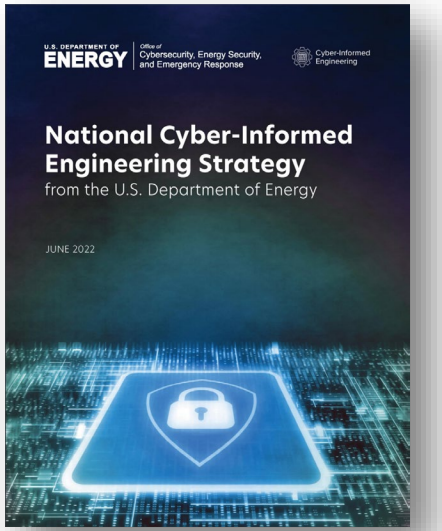
Cyber-Informed Engineering

Cyber-Informed Engineering (CIE)

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability
- CIE aims to create a **culture of security** aligned with the existing industry safety culture

National CIE Strategy

- Directed by the U.S. Congress in the Fiscal Year 2020 National Defense Authorization Act
- Outlines core CIE concepts
  - Defined by a set of design, operational, and organizational principles
  - Placed cybersecurity considerations at the foundation of control systems design and engineering

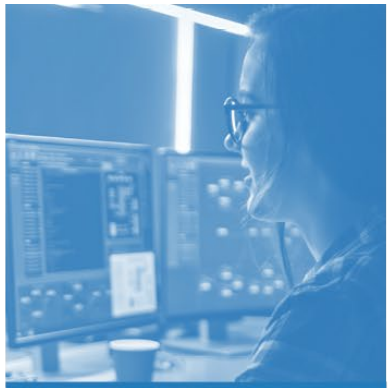

U.S. DEPARTMENT OF ENERGY
Office of Cybersecurity, Energy Security, and Emergency Response
Cyber-Informed Engineering
National Cyber-Informed Engineering Strategy
from the U.S. Department of Energy
JUNE 2022

https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

Pillars of the National CIE Strategy

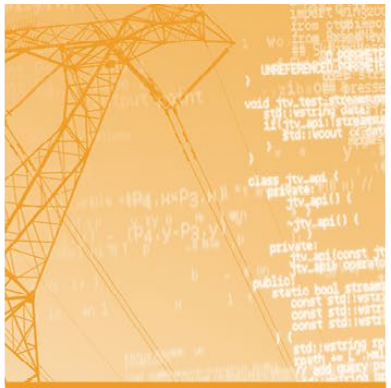
Awareness

Promulgate a universal and shared understanding of CIE



Education

Embed CIE into formal education, training, and credentialing



Development

Build the body of knowledge by which CIE is applied to specific implementations

Current Infrastructure

Apply CIE principles to existing systemically important critical infrastructure

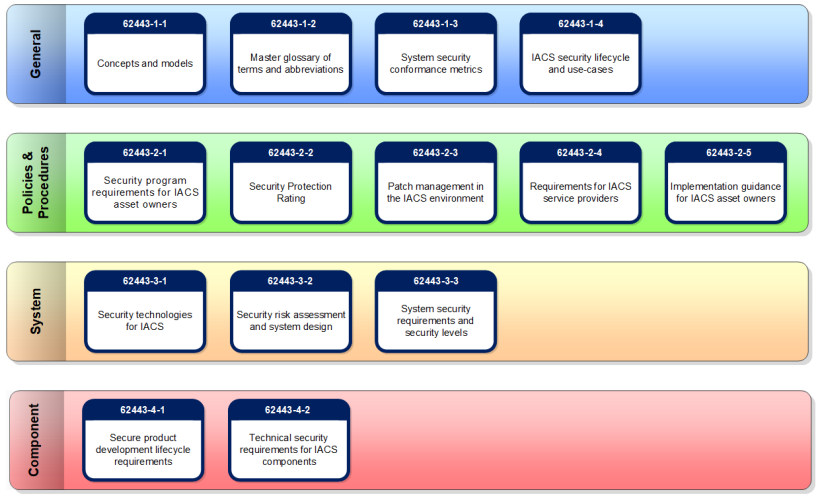
Future Infrastructure

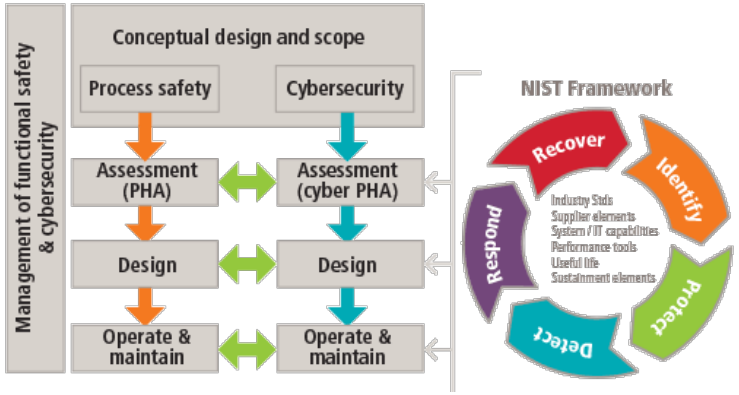
Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology

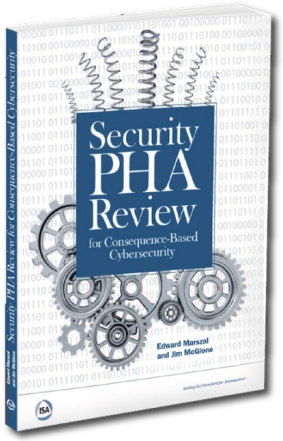
CIE Principles

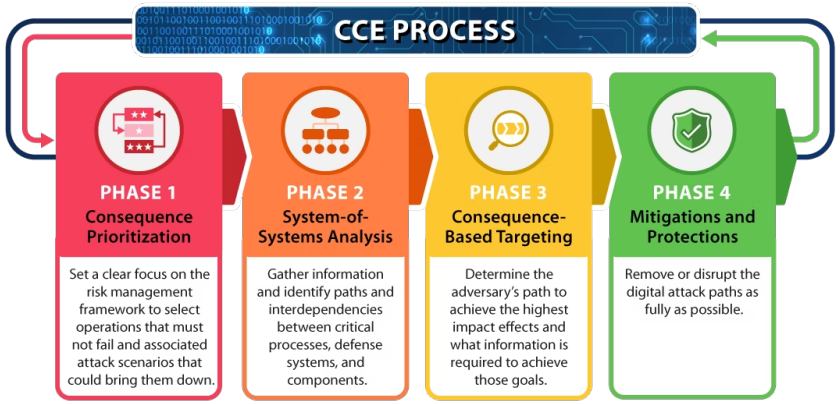
Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security we need?
Planned Resilience	How do I turn “what ifs” into “even ifs”?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

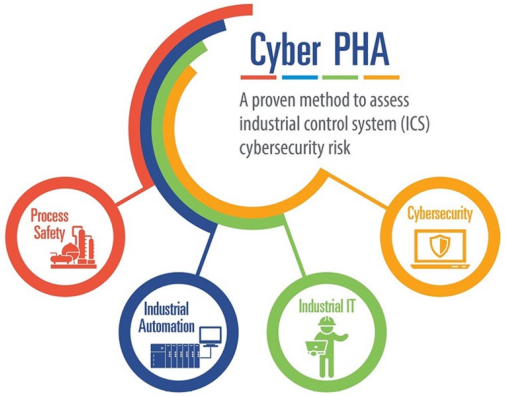
OK, But How Do You CIE?





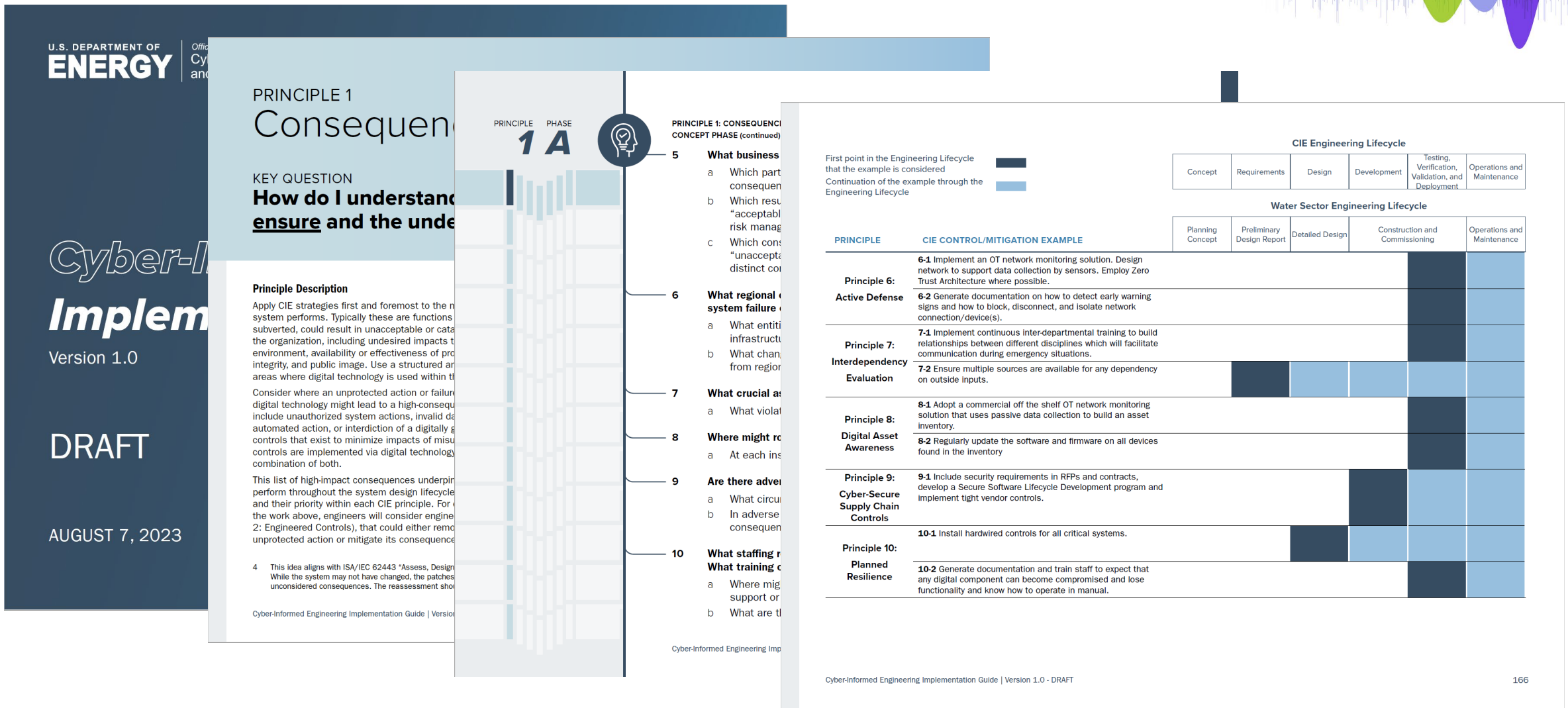



CCE PROCESS
PHASE 1
Consequence Prioritization
Set a clear focus on the risk management framework to select operations that must not fail and associated attack scenarios that could bring them down.
PHASE 2
System-of-Systems Analysis
Gather information and identify paths and interdependencies between critical processes, defense systems, and components.
PHASE 3
Consequence-Based Targeting
Determine the adversary's path to achieve the highest impact effects and what information is required to achieve those goals.
PHASE 4
Mitigations and Protections
Remove or disrupt the digital attack paths as fully as possible.



CIE and the Systems Engineering Lifecycle

CIE Implementation Guide



U.S. DEPARTMENT OF ENERGY

Cyber-I

Implem

Version 1.0

DRAFT

AUGUST 7, 2023

PRINCIPLE 1

Consequen

KEY QUESTION

How do I understand

ensure and the unde

Principle Description

Apply CIE strategies first and foremost to the n
system performs. Typically these are functions
subverted, could result in unacceptable or cata
the organization, including undesired impacts t
environment, availability or effectiveness of pro
integrity, and public image. Use a structured ar
areas where digital technology is used within th

Consider where an unprotected action or failure
digital technology might lead to a high-consequ
include unauthorized system actions, invalid da
automated action, or interdiction of a digitally g
controls that exist to minimize impacts of misu
controls are implemented via digital technology
combination of both.

This list of high-impact consequences underpin
perform throughout the system design lifecycle
and their priority within each CIE principle. For
the work above, engineers will consider engine
2: Engineered Controls), that could either remo
unprotected action or mitigate its consequence

4 This idea aligns with ISA/IEC 62443 "Assess, Design
While the system may not have changed, the patches
unconsidered consequences. The reassessment sho

Cyber-Informed Engineering Implementation Guide | Versio

PRINCIPLE 1 A

PRINCIPLE 1: CONSEQUENCI
CONCEPT PHASE (continued)

5 **What business**
- a Which part
consequen
- b Which resu
"acceptabl
risk manag
- c Which cons
"unaccepta
distinct co

6 **What regional**
system failure
- a What entiti
infrastructu
- b What chan
from regio

7 **What crucial a**
- a What violat

8 **Where might r**
- a At each ins

9 **Are there adve**
- a What circu
- b In adverse
consequen

10 **What staffing**
What training
- a Where mig
support or
- b What are t

Cyber-Informed Engineering Imp

First point in the Engineering Lifecycle that the example is considered

Continuation of the example through the Engineering Lifecycle

CIE Engineering Lifecycle

Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance

Water Sector Engineering Lifecycle

Planning Concept	Preliminary Design Report	Detailed Design	Construction and Commissioning	Operations and Maintenance

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE
Principle 6: Active Defense	**6-1** Implement an OT network monitoring solution. Design network to support data collection by sensors. Employ Zero Trust Architecture where possible.
	6-2 Generate documentation on how to detect early warning signs and how to block, disconnect, and isolate network connection/device(s).
Principle 7: Interdependency Evaluation	**7-1** Implement continuous inter-departmental training to build relationships between different disciplines which will facilitate communication during emergency situations.
	7-2 Ensure multiple sources are available for any dependency on outside inputs.
Principle 8: Digital Asset Awareness	**8-1** Adopt a commercial off the shelf OT network monitoring solution that uses passive data collection to build an asset inventory.
	8-2 Regularly update the software and firmware on all devices found in the inventory
Principle 9: Cyber-Secure Supply Chain Controls	**9-1** Include security requirements in RFPs and contracts, develop a Secure Software Lifecycle Development program and implement tight vendor controls.
Principle 10: Planned Resilience	**10-1** Install hardwired controls for all critical systems.
	10-2 Generate documentation and train staff to expect that any digital component can become compromised and lose functionality and know how to operate in manual.

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT 166

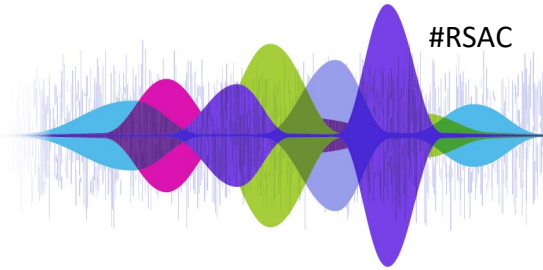
https://www.osti.gov/servlets/purl/1995796

RSAC 2025 Conference

How Does This Work In Practice?

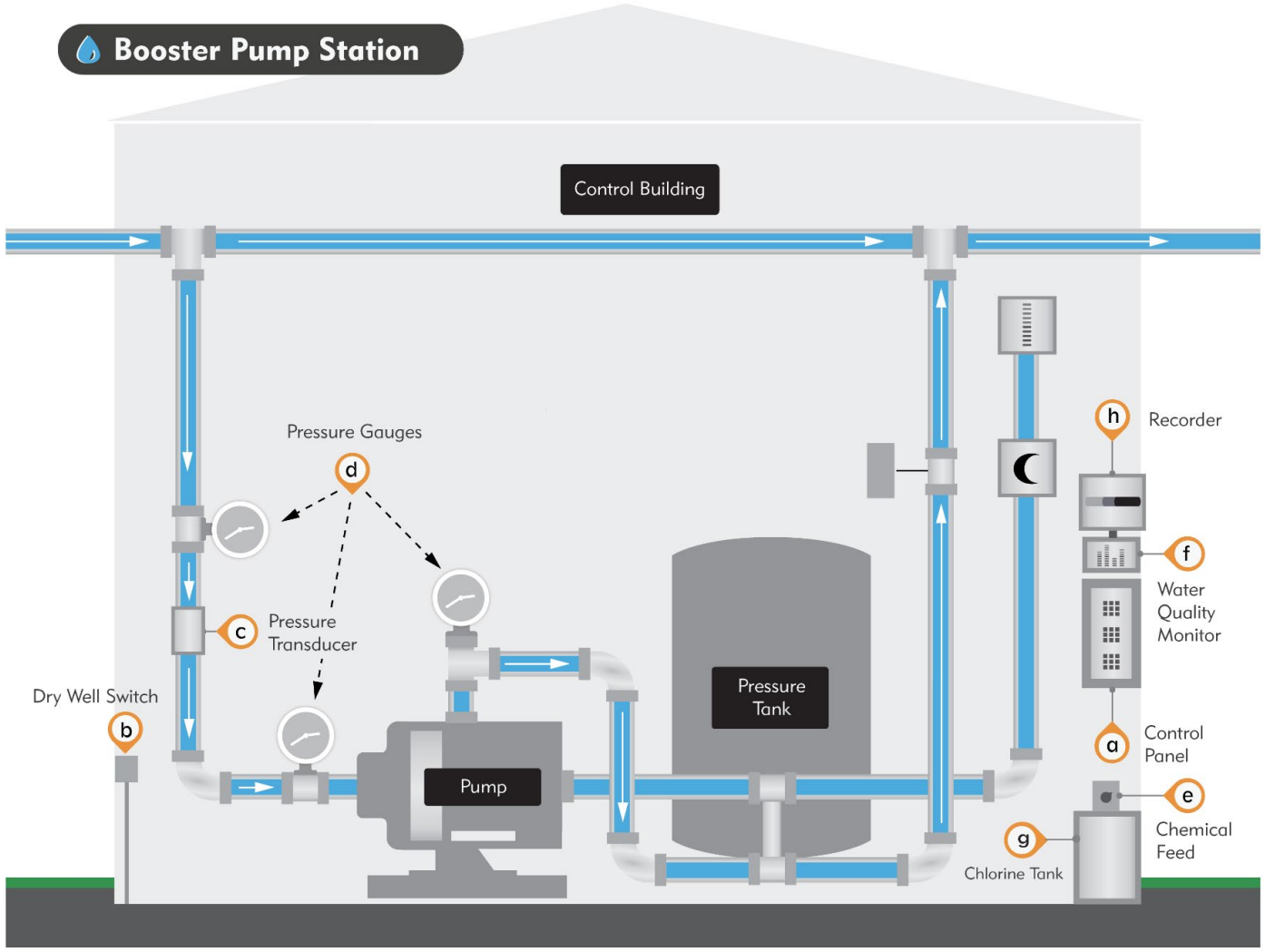
…especially for municipal utilities…

Application Of CIE To Municipal Utilities



- Identify high-consequence cyber risks to critical systems, treating these risks in the same manner as mechanical stress, electrical faults, weather/environment impacts, or material failures
- Design critical systems with resilience in mind and to minimize the impact of potential cyber incidents
  - Implement network segmentation to isolate OT and ICS systems from IT systems
  - Implement robust authentication and access control with MFA
  - Include fail-safe mechanical overrides for any digitally control system
- Create a culture of security and train employees to recognize potential cyber risks

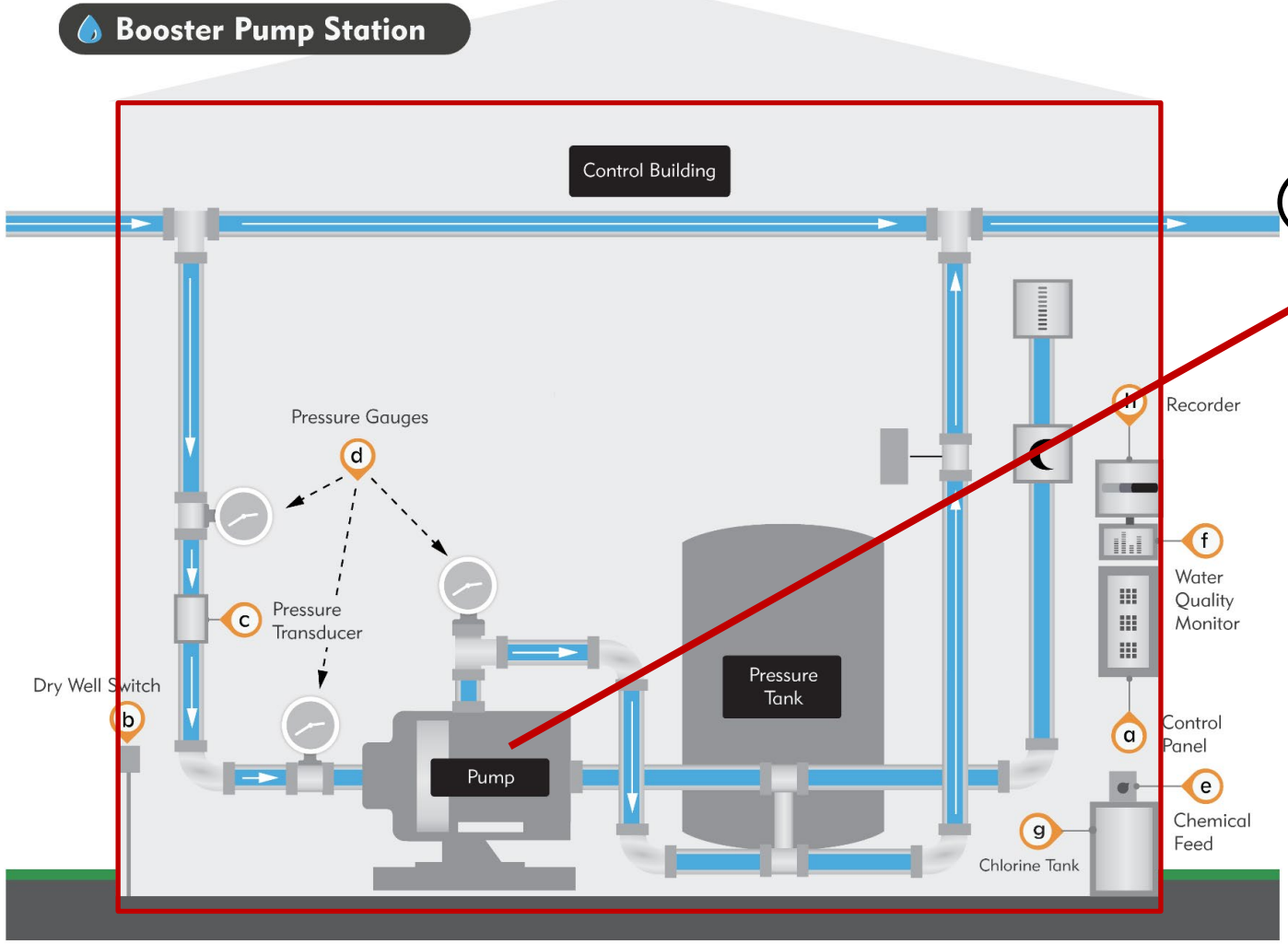
Example: Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://bmxlovesk.xyz/product_details/13200675.html

Example: Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://bmxlovesk.xyz/product_details/13200675.html

Cyber Solution Review

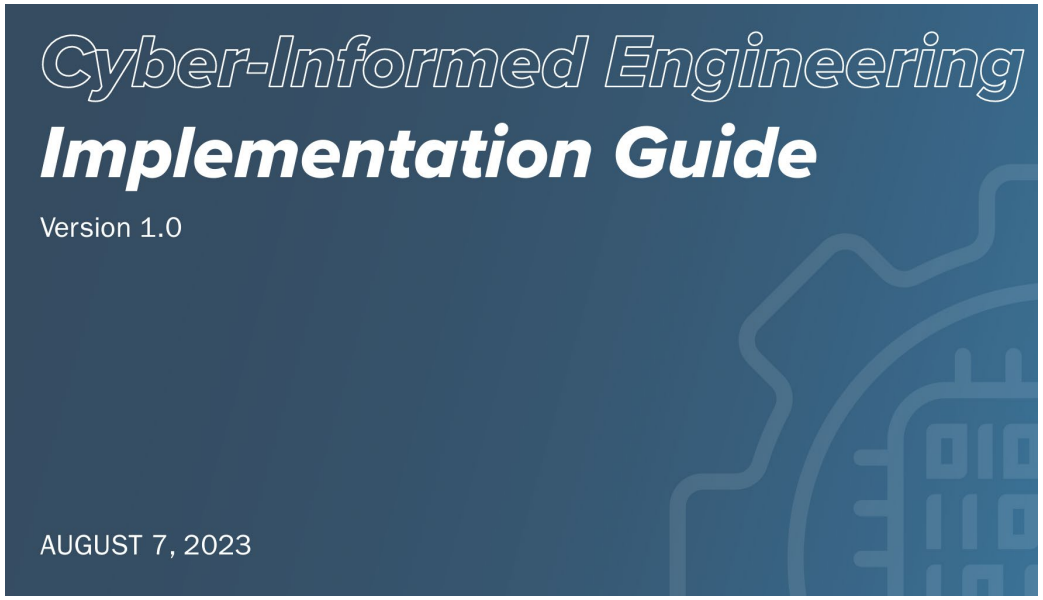
- Control System Software has a qualifying secure development lifecycle
  - Very mature demonstrated processes
  - Provided SBOM
  - Component infrastructure is up to date
  - Mature vulnerability release process – with regular patches
  - 24/7 support availability
- Cloud provider is reputable and qualified
  - SOC Type 2 and Fedramp (if needed), great physical security
  - Very mature, experienced in hosting critical infrastructure services
  - Demonstrated response and restoration capabilities

IT Installation Review

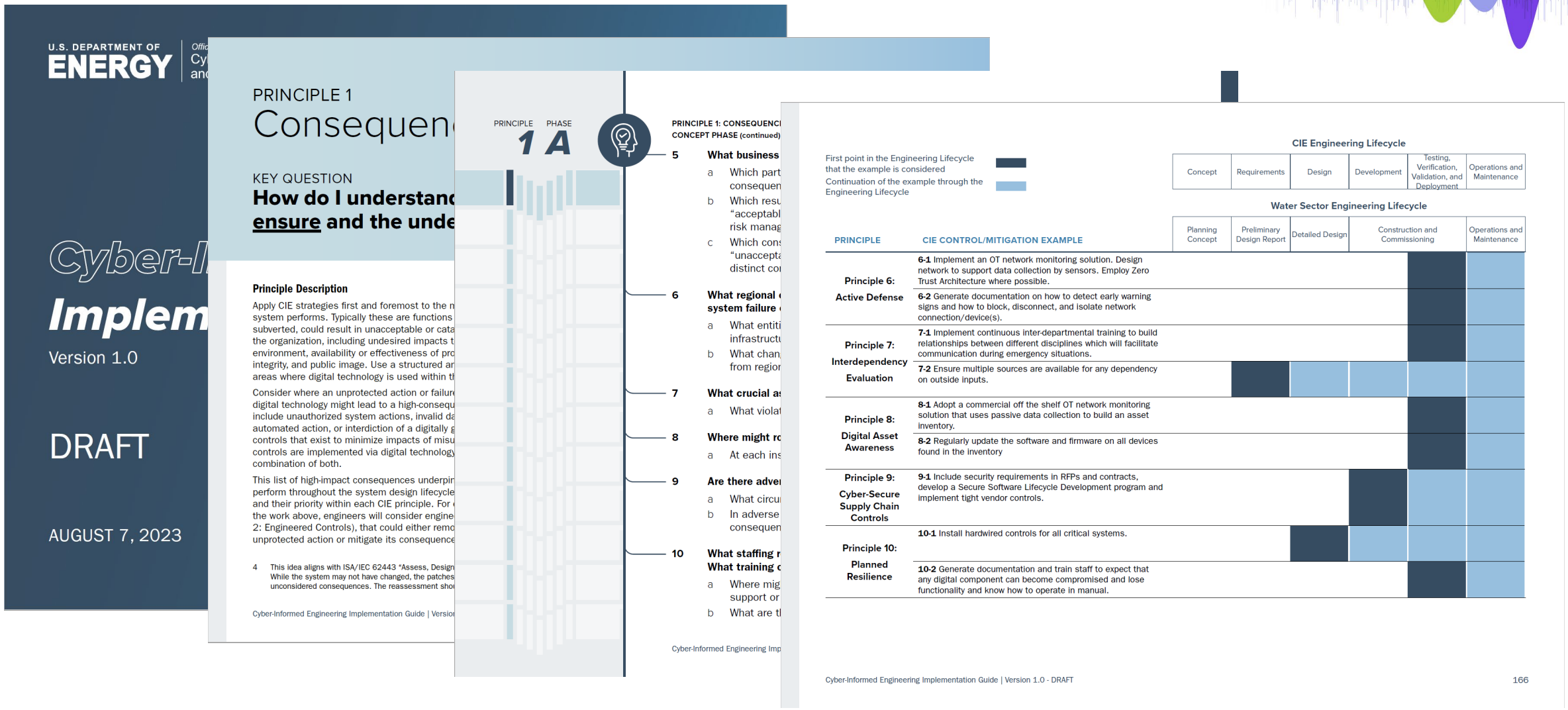
- Network entry point has standard security package
- Monitoring and logging traffic on this interface conforms with standard practices
  - Logging interfaces with organizational logging system
- Traffic in and out is encrypted between the cloud provider and the internal network boundary

Organizational Review Board Votes

- Finance / Accounting – ☑
- Information Technology – ☑
- Cybersecurity – ☑
- Engineering Operations – ? ➡



CIE Implementation Guide



U.S. DEPARTMENT OF ENERGY

Cyber-I

Implem

Version 1.0

DRAFT

AUGUST 7, 2023

PRINCIPLE 1

Consequen

KEY QUESTION

How do I understand

ensure and the unde

Principle Description

Apply CIE strategies first and foremost to the n
system performs. Typically these are functions
subverted, could result in unacceptable or cata
the organization, including undesired impacts t
environment, availability or effectiveness of pro
integrity, and public image. Use a structured ar
areas where digital technology is used within th

Consider where an unprotected action or failure
digital technology might lead to a high-consequ
include unauthorized system actions, invalid da
automated action, or interdiction of a digitally g
controls that exist to minimize impacts of misu
controls are implemented via digital technology
combination of both.

This list of high-impact consequences underpin
perform throughout the system design lifecycle
and their priority within each CIE principle. For
the work above, engineers will consider engine
2: Engineered Controls), that could either remo
unprotected action or mitigate its consequence

4 This idea aligns with ISA/IEC 62443 "Assess, Design
While the system may not have changed, the patches
unconsidered consequences. The reassessment sho

Cyber-Informed Engineering Implementation Guide | Versio

PRINCIPLE 1 A

PRINCIPLE 1: CONSEQUENCI
CONCEPT PHASE (continued)

5 **What business**
- a Which part
consequen
- b Which resu
"acceptabl
risk manag
- c Which cons
"unaccepta
distinct co

6 **What regional**
system failure
- a What entiti
infrastructu
- b What chan
from regio

7 **What crucial a**
- a What violat

8 **Where might r**
- a At each ins

9 **Are there adve**
- a What circu
- b In adverse
consequen

10 **What staffing**
What training
- a Where mig
support or
- b What are t

Cyber-Informed Engineering Imp

First point in the Engineering Lifecycle that the example is considered

Continuation of the example through the Engineering Lifecycle

CIE Engineering Lifecycle

Concept	Requirements	Design	Development	Testing, Verification, Validation, and Deployment	Operations and Maintenance

Water Sector Engineering Lifecycle

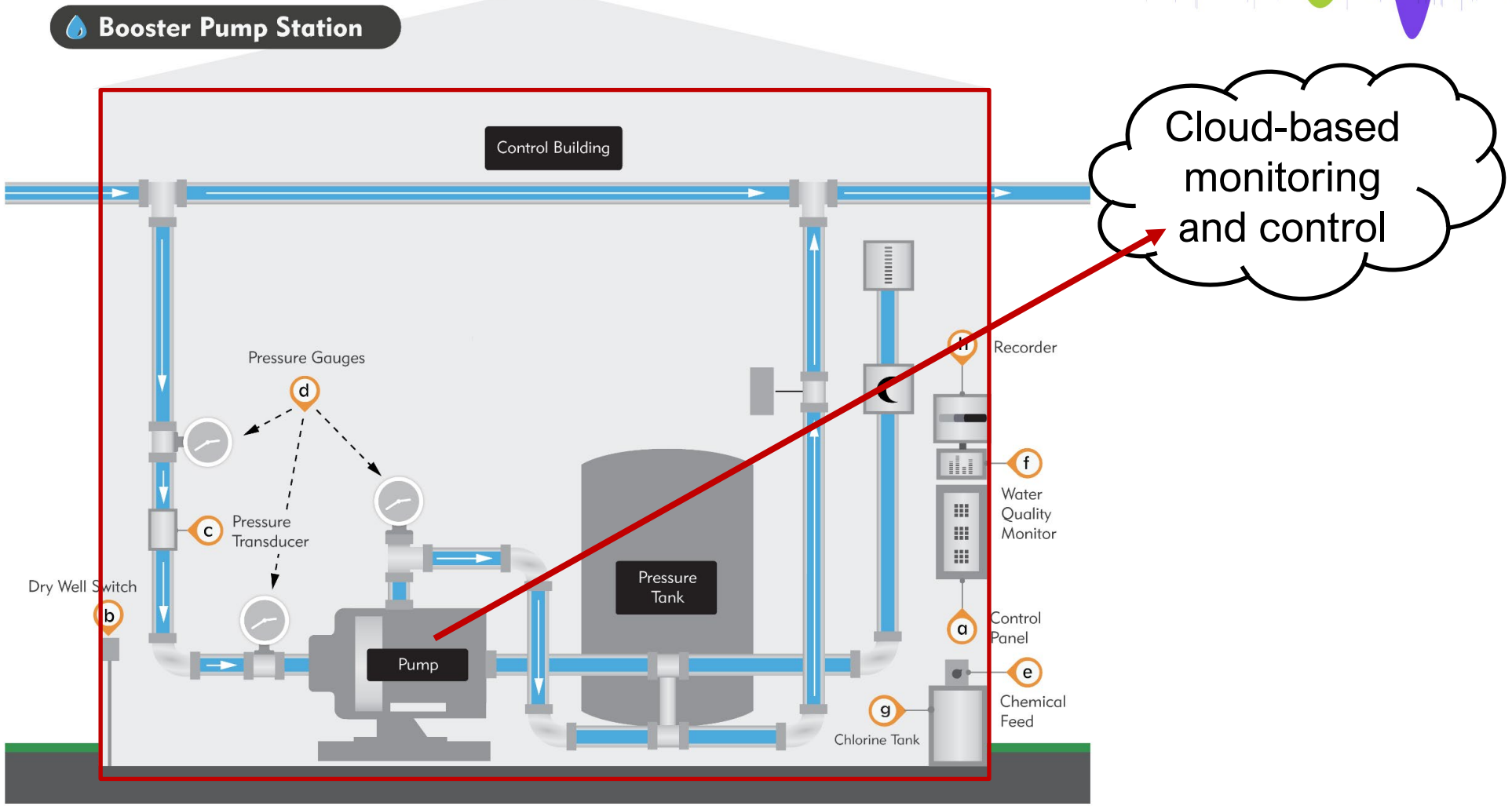
Planning Concept	Preliminary Design Report	Detailed Design	Construction and Commissioning	Operations and Maintenance

PRINCIPLE	CIE CONTROL/MITIGATION EXAMPLE
Principle 6: Active Defense	**6-1** Implement an OT network monitoring solution. Design network to support data collection by sensors. Employ Zero Trust Architecture where possible.
	6-2 Generate documentation on how to detect early warning signs and how to block, disconnect, and isolate network connection/device(s).
Principle 7: Interdependency Evaluation	**7-1** Implement continuous inter-departmental training to build relationships between different disciplines which will facilitate communication during emergency situations.
	7-2 Ensure multiple sources are available for any dependency on outside inputs.
Principle 8: Digital Asset Awareness	**8-1** Adopt a commercial off the shelf OT network monitoring solution that uses passive data collection to build an asset inventory.
	8-2 Regularly update the software and firmware on all devices found in the inventory
Principle 9: Cyber-Secure Supply Chain Controls	**9-1** Include security requirements in RFPs and contracts, develop a Secure Software Lifecycle Development program and implement tight vendor controls.
Principle 10: Planned Resilience	**10-1** Install hardwired controls for all critical systems.
	10-2 Generate documentation and train staff to expect that any digital component can become compromised and lose functionality and know how to operate in manual.

Cyber-Informed Engineering Implementation Guide | Version 1.0 - DRAFT 166

https://www.osti.gov/servlets/purl/1995796

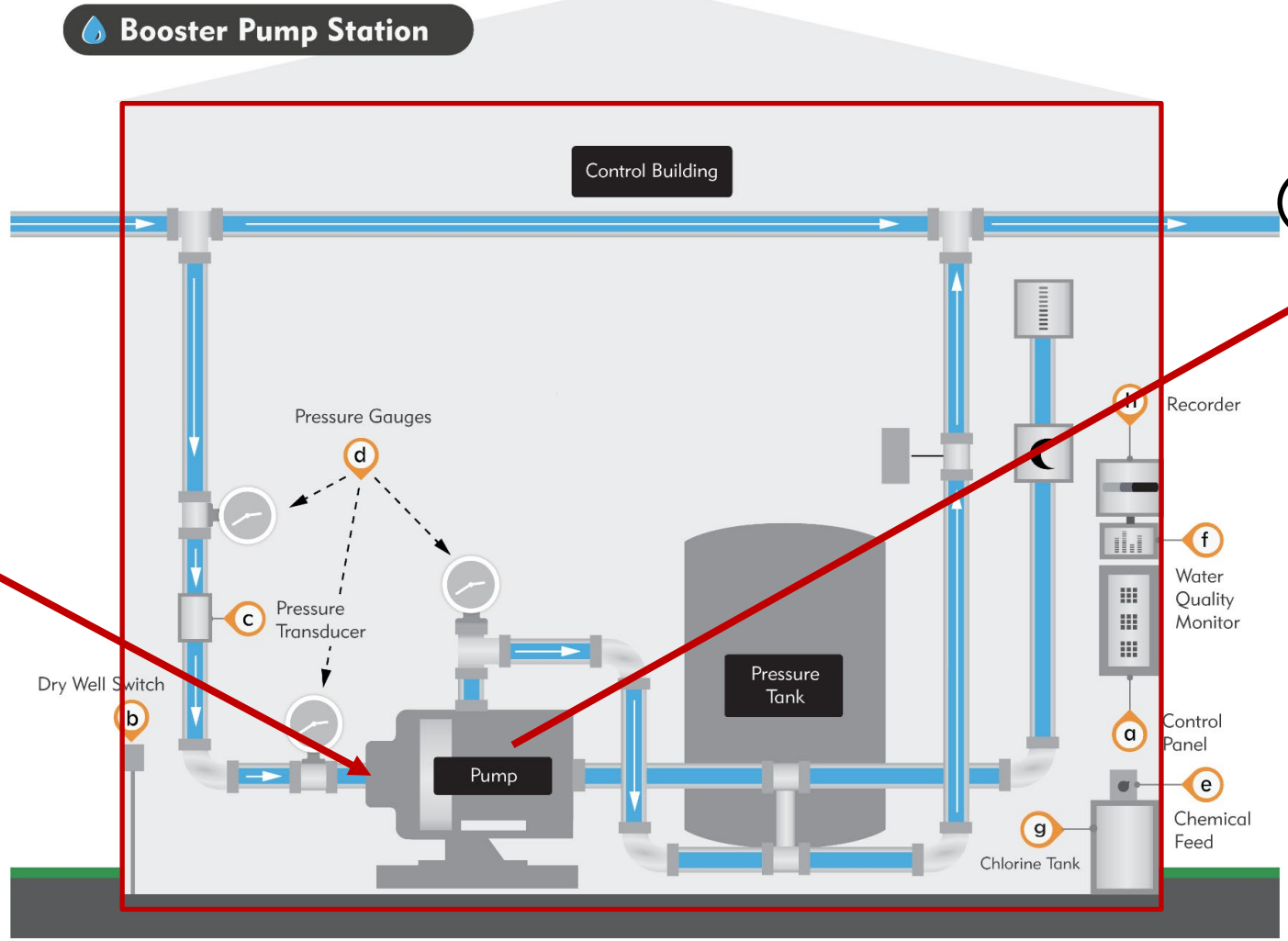
Water Booster Pump Station



Water Booster Pump Station Archives App4Water

https://bmxlovesk.xyz/product_details/13200675.html

Water Booster Pump Station



Water Booster Pump Station Archives App4Water

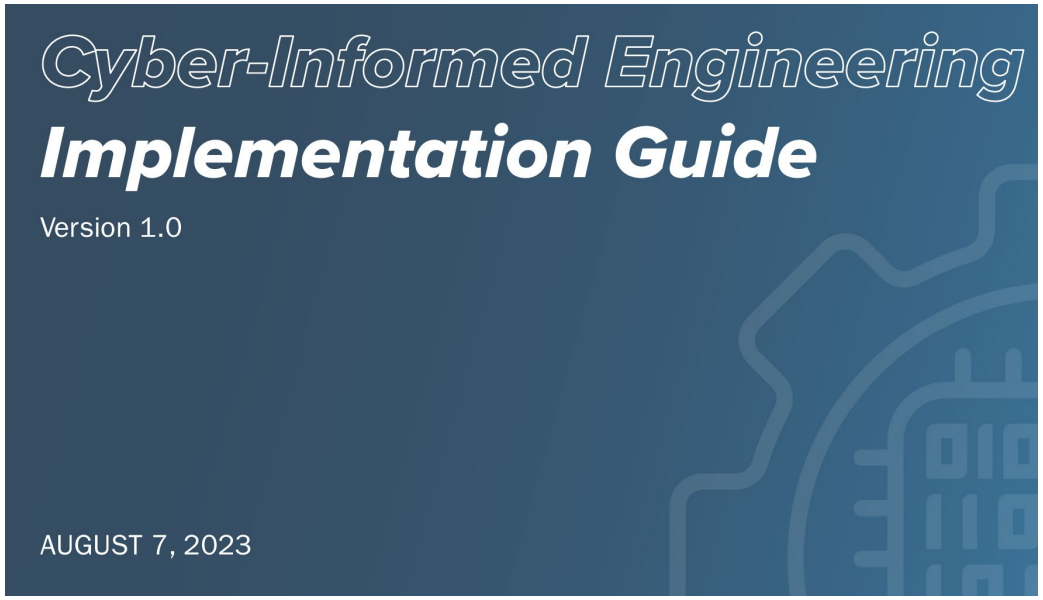
Cloud-based monitoring and control

Mechanical Time Delay Relay

https://bmxlovesk.xyz/product_details/13200675.html

Organizational Review Board Votes

- Finance / Accounting – ☑
- Information Technology – ☑
- Cybersecurity – ☑
- Engineering Operations – ☑ ➡



RSAC™ 2025 Conference

How To Get Involved With Cyber-Informed Engineering

CIE Community of Practice and Working Groups

Cyber-Informed Engineering COP

Quarterly

11 AM ET on the 2nd Wednesday of January, April, July, and October

Multi-stakeholder team to aid the translation of CIE into technical requirements that can inform guidance, practices, and standards development

CIE Standards WG

Monthly

1st Wednesday, 9 AM MT / 11 AM ET

Support integration of CIE into engineering and cybersecurity standards

CIE Education WG

Monthly

3rd Wednesday, 9 AM MT / 11 AM ET

Develop curricula and materials that integrate CIE principles into engineering degree programs

CIE Implementation WG

Monthly

4th Wednesday, 9 AM MT / 11 AM ET

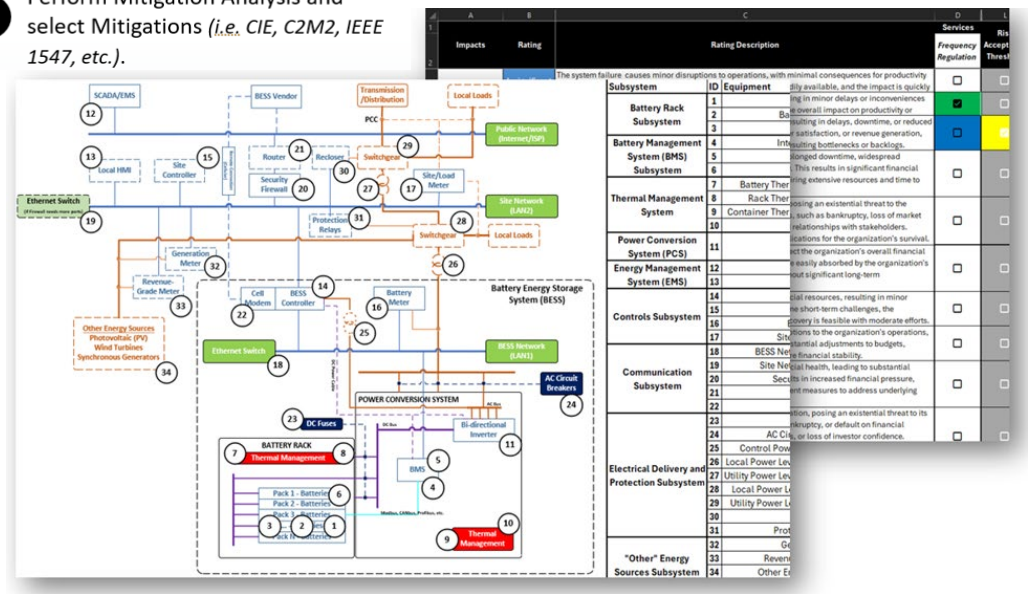
Develop CIE implementation guidance and an open-source library of resources

CIE Tools – Battery and Microgrid

- Open Source tools applying CIE
- For Microgrids and Battery Energy Storage Systems
- **CIEMAT** – CIE for Microgrids Tool - https://github.com/idaholab/CIEMAT/tree/main
- **CIEBAT** – CIE for Battery Energy Storage Systems Tool - https://github.com/idaholab/CIEBAT/tree/main

Steps in the Template

1. Detail and Describe the System Characteristics *(i.e., BESS, PV, Generators, IBR Resources, etc.)*
2. Select Grid Services Provided *(i.e., Backup Power, Voltage Regulation, etc.)* and describe how the System provides Grid Service(s). *(i.e., Enabling Functions)*
3. Determine Consequence Threshold (Impact Rating)
4. Perform Consequence Analysis from both Engineering and Cybersecurity perspective.
5. Perform Mitigation Analysis and select Mitigations *(i.e. CIE, C2M2, IEEE 1547, etc.)*.



Additional CIE Information

- Websites
  - DOE CESER -- https://www.energy.gov/ceser/cyber-informed-engineering
  - INL - https://inl.gov/cie/
  - NREL - https://www.nrel.gov/security-resilience/cyber-informed-engineering.html
- CIE Publications
  - Implementation Guide: https://www.osti.gov/biblio/1995796
  - Workbook for ADMS: https://www.osti.gov/biblio/1986517
  - Workbook for Microgrids: https://www.osti.gov/biblio/2315001
  - Workbook for Water Systems: https://www.osti.gov/biblio/2371031
  - Analysis Tool: https://github.com/inlguy/CIE/releases/tag/v12.2.4.0

“Apply” Slide

- Next week you should:
  - Identify critical infrastructures or services within your organization
- In the first three months following this presentation you should:
  - Identify potential cyber risks and consequences, from where and why
  - Define appropriate engineering controls to mitigate these risks
- Within six months you should:
  - Select engineered solutions that will achieve desired consequence mitigation
  - Drive an implementation project to protect all critical systems

RSAC 2025 Conference

Many Voices.
One Community.

Thank You!

https://www.energy.gov/ceser/cyber-informed-engineering

CIE@inl.gov